

Exhibit 31

1 of 11 DOCUMENTS

Copyright 2005 CMP Media LLC
InformationWeek

November 21, 2005

SECTION: NEWS & ANALYSIS; Pg. 28

LENGTH: 791 words

HEADLINE: Sony Plays The Blues As Bloggers Turn Up The Volume -- Company halts sales of CDs with content-protection software after complaints

BYLINE: Thomas Claburn with Gregg Keizer

HIGHLIGHT:

After two weeks of withering criticism from bloggers and others, Sony BMG Music Entertainment last week found itself forced to stop selling some 50 CD titles with its Extended Copy Protection content-protection software, remove the discs from stores, and offer replacements without copy protection to customers.

BODY:

Sony issued an apology on its Web site, citing security concerns raised by installation of the XCP software, provided-as Sony was quick to point out-by digital-rights-management vendor First4Internet Ltd.

"We share the concerns of consumers regarding these discs," the company said in a statement. Sony instructed retailers to remove unsold CDs with XCP software from their store shelves and inventory. But the trouble isn't over: The company faces charges of deceptive advertising, illegal spyware distribution, and computer crimes in three lawsuits.

Since Oct. 31, when security researcher Mark Russinovich first posted on his blog that Sony's music CDs surreptitiously installed digital-rights-management software based on a rootkit-software often synonymous with spyware-bloggers of all stripes, from seasoned security experts to aggrieved consumers, fumed about the record company's unethical and possibly illegal behavior.

Thomas Hesse, president of Sony BMG's Global Digital Business, attempted at first to downplay the controversy. "Most people, I think, don't even know what a rootkit is, so why should they care about it?" he said, in a Nov. 4 interview with National Public Radio. The software, Hesse explained, was designed to protect Sony's CDs from unauthorized copying and ripping.

Two days earlier, Sony tried to mollify critics by offering an update that removed what it called "the cloaking technology component" of XCP. The notes to that update state the component was "not malicious and does not compromise security." That may be true, but another component, the uninstaller provided by Sony to remove the XCP software, did compromise security, and bloggers were quick to jump on that, too.

Defensive Stance

The music industry has been torn between protecting its assets and not alienating the public. At a music industry conference in San Diego last summer, Recording Industry Association of America CEO Mitch Bainwol presented findings by market-research firm NPD Group that suggested ripping songs-copying them to a computer from a CD-has come to represent a revenue threat that's at least as significant as illegal peer-to-peer file trading.

Security-software companies and Microsoft are responding to the Sony problem with tools to detect and remove the rootkit, which might be found in business environments if employees played the Sony CDs on office PCs. Microsoft plans to update its Windows AntiSpyware software and Windows Live Safety Center, a free, online antivirus service, to dig out the rootkit. Next month, Microsoft also will add the Sony rootkit to the worms, Trojans, and viruses detected and deleted by Windows Malicious Software Removal Tool, which is updated the second Tuesday of each month.

Sony Plays The Blues As Bloggers Turn Up The Volume -- Company halts sal

The incident isn't comparable to a virus attack in terms of impact, according to Graham Cluley, senior technology consultant with security company Sophos plc. "Sony's code wasn't intentionally malicious, but did open up a security hole on users' computers which could be exploited by malware," Cluley says via E-mail.

But the rootkit is by no means benign. It can be used by attackers to hide malicious code, and at least two Trojan horses for that purpose already have been spotted. "Rather than malware," says Cluley, "I would term this as 'ineptware.'" -THOMAS CLABURN (tclaburn @cmp.com), with GREGG KEIZER

From The Blogosphere

"Not only had Sony put software on my system that uses techniques commonly used by malware to mask its presence, the software is poorly written and provides no means for uninstall. Worse, most users ... will cripple their computer if they attempt the obvious step of deleting the cloaked files." -Mark Russinovich's Oct. 31 posting on Mark's Sysinternals Blog, <http://www.sysinternals.com/Blog>

"The First4Internet XCP copy protection software. ... allows any web page you visit to download, install, and run any code it likes on your computer. ... That's about as serious as a security flaw can get." -J. Alex Halderman and Ed Felten's Nov. 15 posting on Freedom To Tinker, <http://www.freedom-to-tinker.com>

Sony is "getting away with the whole incident, with only some PR damage that they've turned around to look like as if the whole problem was just a security flaw." -Matti Nikki's Nov. 18 posting at hack.fi/muzzy/sony-drm/rant-and-whine.html

<http://informationweek.com/>

Copyright (c) 2005 CMP Media LLC. All rights reserved.

LOAD-DATE: November 21, 2005